Public Health Information Network Messaging System

A Standards Based Approach to Message Transport

M. Barry Rhodes, Ph.D.

Associate Director for Public Health Systems Development, IRMO, CDC

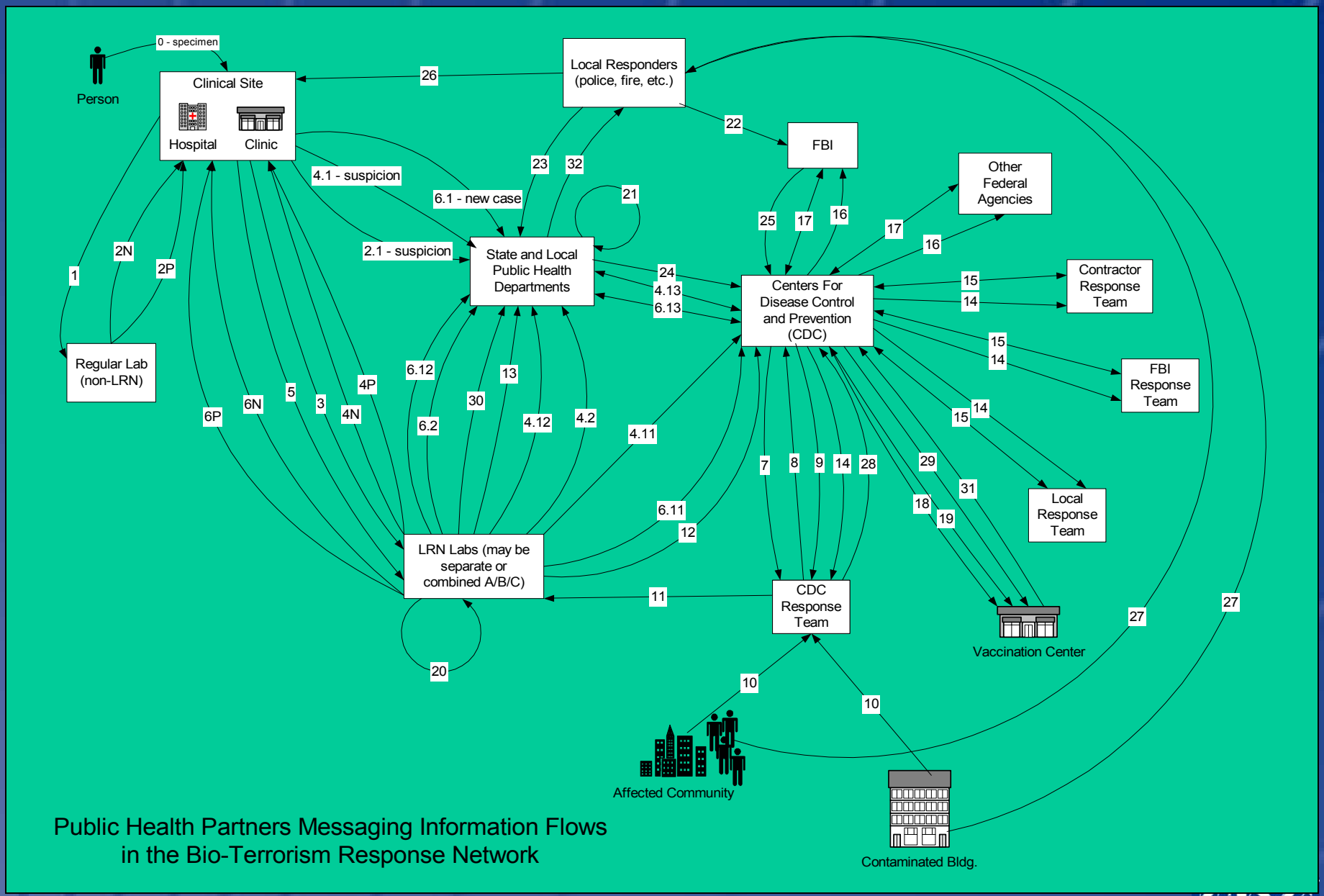
PHINMS Vision

- Standards not software
- Interoperability across vendors, platforms, and jurisdictions
- A network where messages can be easily exchanged between labs, hospitals, physicians, researchers, public heath officials, emergency responders, federal agencies, and the CDC in a secure, reliable manner

PHIN Standards for Message Transport

- ebXML
- XML DSIG
- XML Encryption
- HTTP(S)
- PKI
- LDAP

Why Do We Need Interoperability?



Public Health Partners Messaging Information Flows in the Bio-Terrorism Response Network

About ebXML

- ebXML enables “a modular yet complete electronic business frame- work for collaborative commerce.” *
- Replacement for EDI
- ebMS used to send all types of files, not just XML
- Specification is jointly sponsored by OASIS and UN/CEFACT

* *Professional ebXML Foundations*, Chappell et. al, Wrox Press, 2001

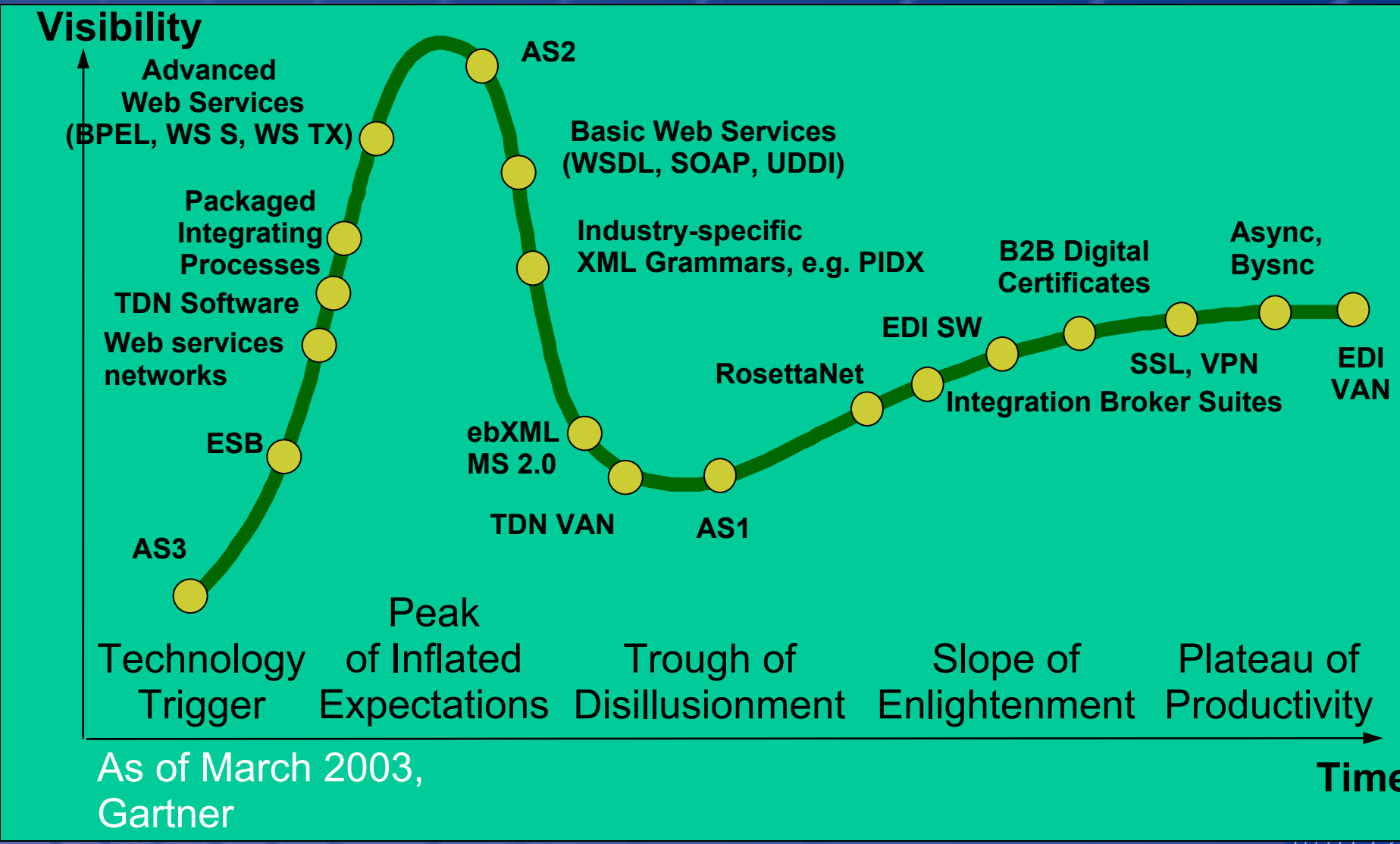
ebXML vs. Web Services

- Not either/or
- ebXML extends Web Services with a directed vocabulary that caters to B2B needs
- If you were to ask how might web services be extended to accommodate B2B electronic commerce. ebXML would be the answer.

Is ebXML the Right Choice for the Public Health Information Network?

- Currently in ballot for adoption by HL7
- Endorsed by Gartner in an evaluation of PHIN standards (see previous presentation)
- See www.ebXML.org

B2B Application Integration Technology Hype Cycle

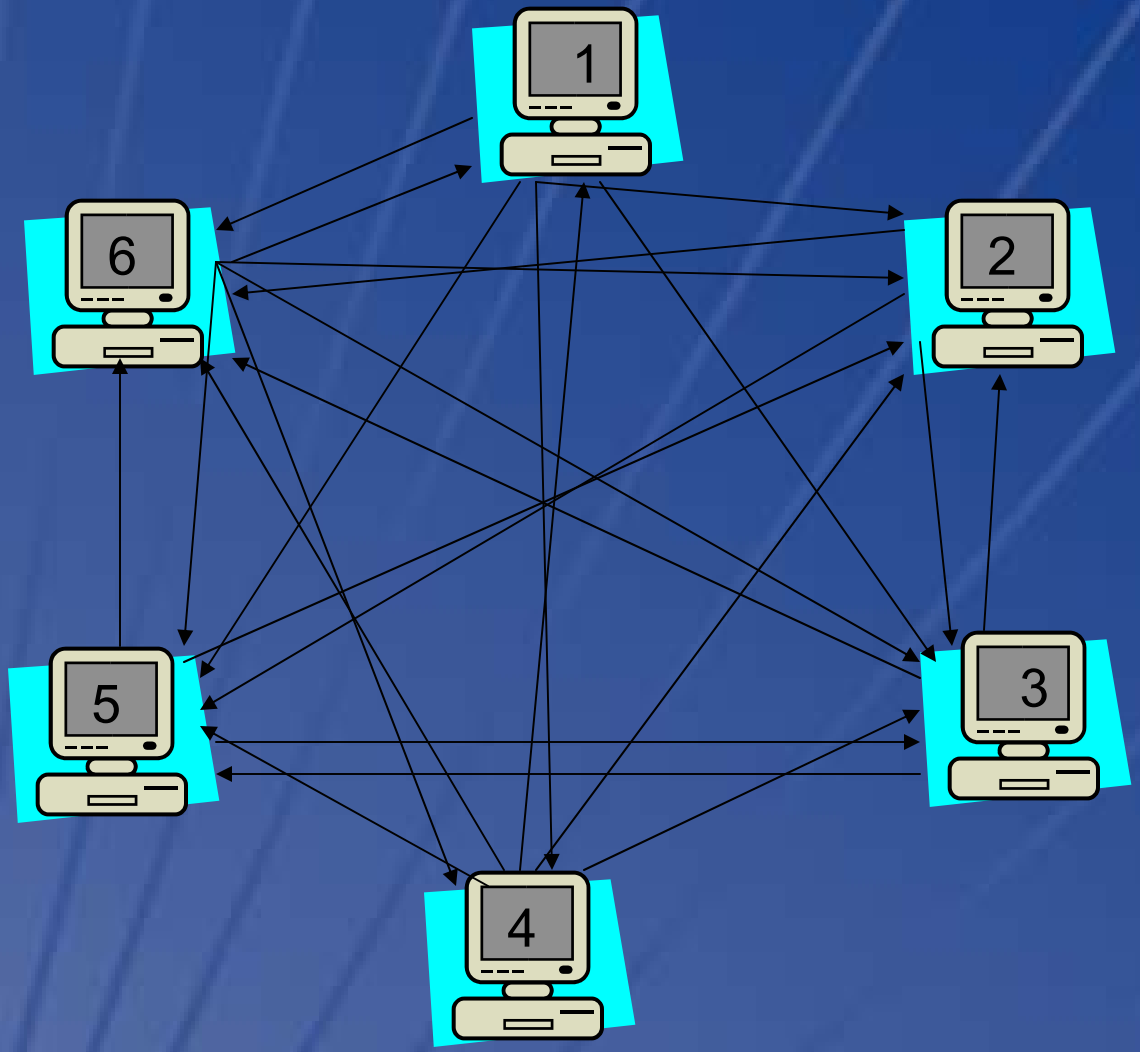


As of March 2003, Gartner

Security Issues

- Security remains a huge stumbling block to the PHINMS vision.
- Transactions between partners are negotiated one by one and stored in a Collaboration Protocol Agreement (CPA)
- SSL is point to point
- No security standards (yet)

N*(N-1) Problem



CDC™

Security Architectures

- Manage N*(N-1) connections
- Route through a central gateway
- Federated identity management, Liberty Alliance, Federal Bridge, eAuthentication Gateway, Passport, wsSecurity, SAML, …..

PHINMS

- CDC's Implementation of the ebXML 2.0 message service standards.
- Java based client and server
- Runs on Windows Unix, Linux
- A separable part of the NEDSS Base System

Interop Testing

- Q3’02 CDC participated in Interop testing with 10 other vendors
- Sponsored by Uniform Code Council (UCC) and hosted by the Drummond Group
- Vendors include Fujitsu, Cyclone, IPNet, Sonic, Sterling, Sun, Sybase, TIBCO and the CDC
- See www.ebusinessready.org/ebxml.html

PHINMS Libraries

- Sun - JDK1.4, J2SDKEE1.3, JSSE, JAXM, Javamail, JavaHelp
- IBM XML Security Suite
- Apache Xerces
- Netscape LDAP SDK
- JDBC drivers (Vendor provided)

PHINMS 2.1 Client

- Capable of sending messages (of any type) from behind firewalls and receiving acks.
- Able to run on a typical workstation as well as a server
- Can poll for messages from a PHINMS 2.1 Server (or other) appropriately configured

PHINMS 2.1 Server

- Runs on a J2EE Application Server configured as a web service
- Able to receive messages at any time
- Supports queue (DBMS table) based interface or custom message handler
- Will support certificate based, password based or SDN authentication

Integration Issues

- Designed to work with any number of integration engines, message translators, or application code.
- Hides all aspects of ebXML
- Queue based interface for sending and receiving.
- Queues are SQL, Oracle, Access, etc tables, or file system

PHINMS Configuration

- Service/Action tag mapped to a message handling service on receiver
- Message handling service can be a web resource (Servlet/JSP/ASP/CGI) or a queue (database table)
- Collaboration Protocol Agreement (CPA)
- Every node needs a CPA with every other node
- Each message hop has an associated CPA
- Describes partner party-ID, end-point, security attributes

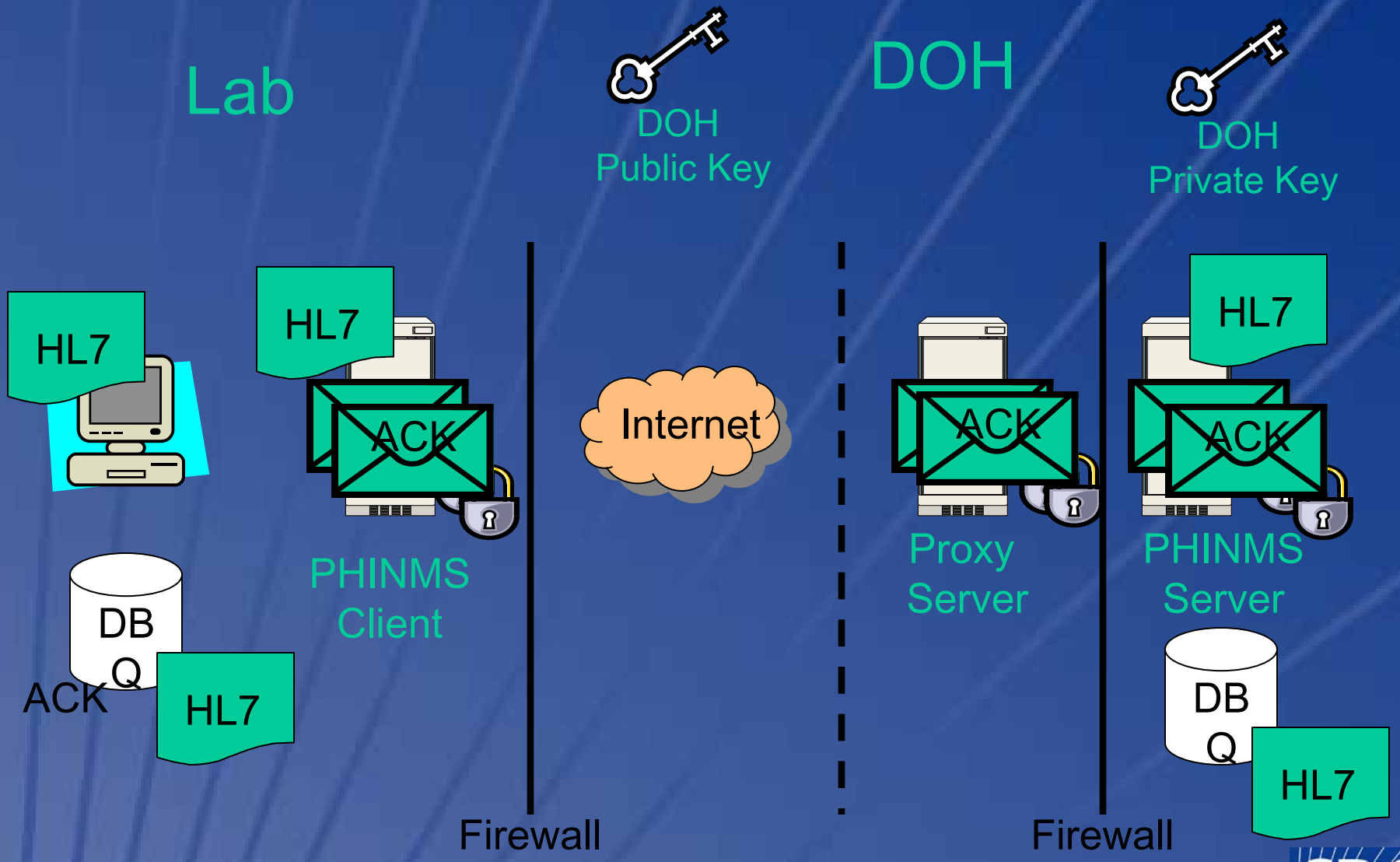
Messaging Topologies

- Direct Send (client/server to server)
- Polling (server to client)
- Route-Not-read (client to client)
- Multi-destination (publish-subscribe, multicast, etc.)

Direct Send

- Single client sends to server
- Optionally encrypt payload with receivers public key
- No intermediary
- Client behind firewall
- Server configured as a web service

Direct Send ELR Example

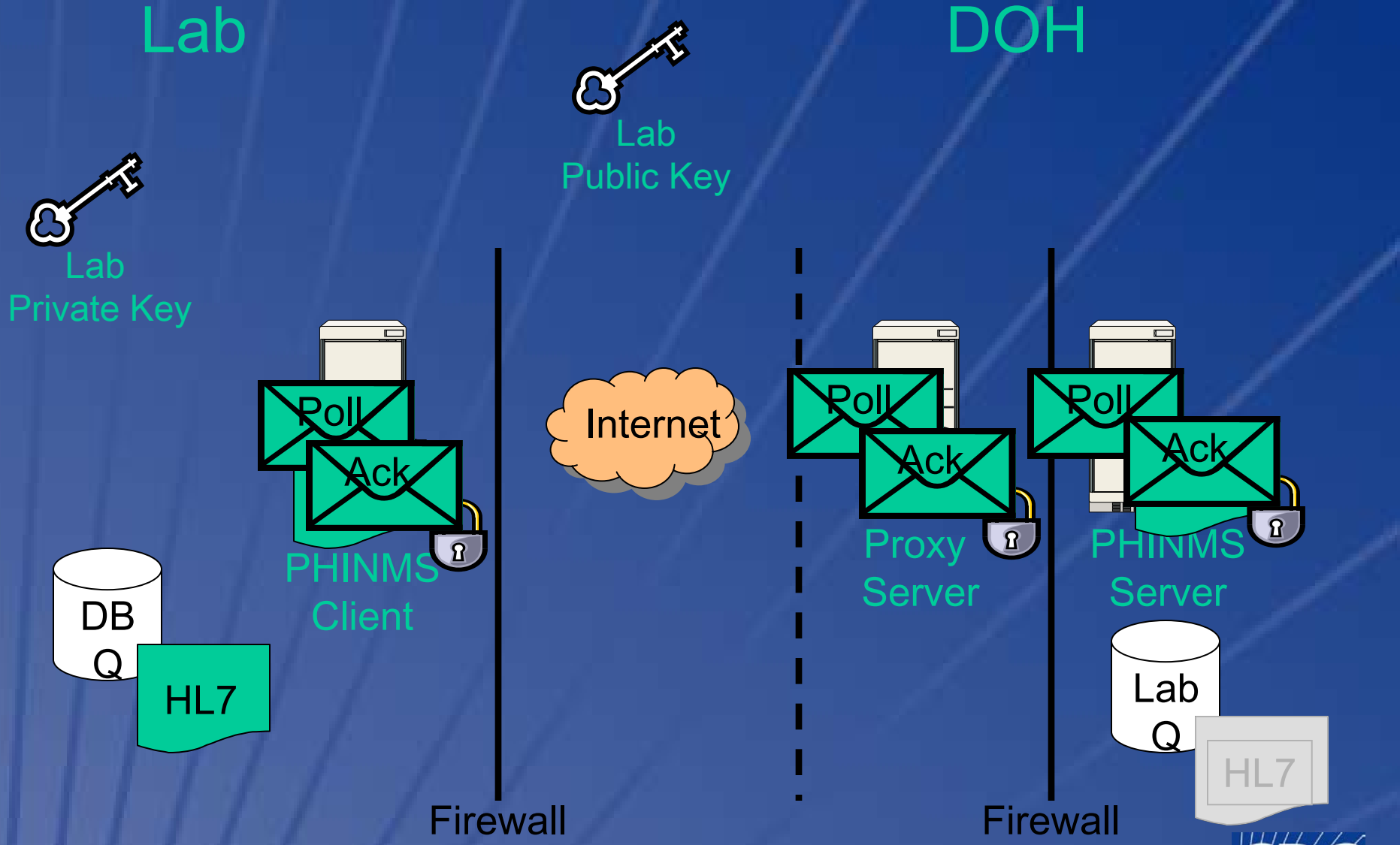


CDC™

Polling

- Server sends to client
- Client polls server for any messages
- Server responds with an acknowledgement with message attached

Polling

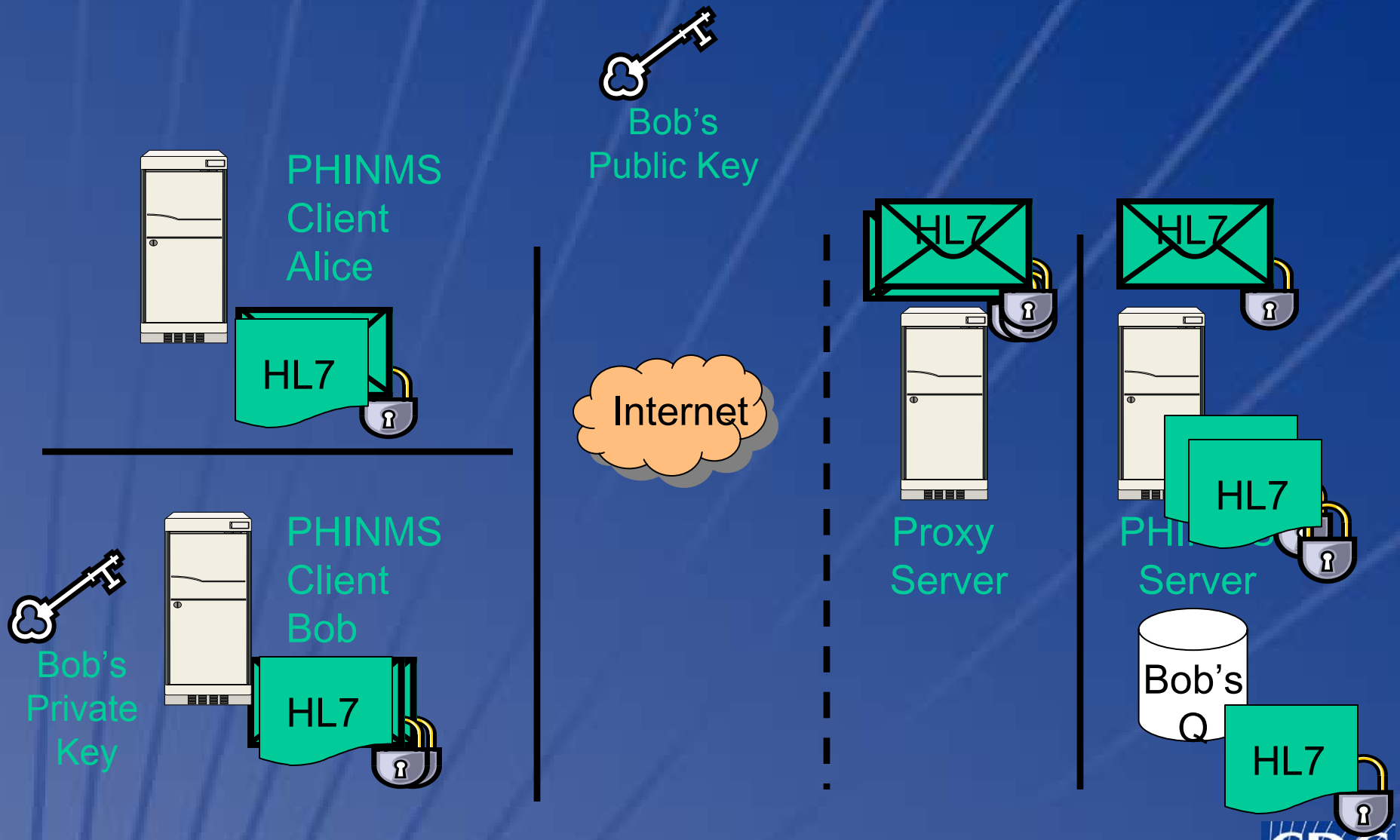

Lab
DOH
Lab
Public Key
Lab
Private Key
Poll
Ack
PHINMS
Client
DB
Q
HL7
Internet
Poll
Ack
Proxy
Server
Poll
Ack
PHINMS
Server
Lab
Q
HL7
Firewall
Firewall

CDC™

Route-Not-Read or Gateway

- Combine direct send and polling to send between two clients.
- Client “A” sends to client “B” via PHINMS Server “C”
- “A” encrypts the message with “B”s public key so that server “C” can never read it

Route-Not-Read Alice sends to Bob



CDC™

Publish Subscribe/ Broadcast

- Message is sent to server with service actions tags that suggest publish to group
- Publisher looks up group subscribers and sends as appropriate
- Working on encryption key issues

Interfacing with PHINMS

- Sending Interface: Simple DB table queue, file directory
- Receiving Interface: Simple DB table queue, file directory, custom written message handler (anything callable from a Java environment) often a servlet

Current Implementations:

- Electronic Lab Reporting from LabCorp to Nebraska DOH
- Nationally Notifiable Disease (NND) messages for Nebraska, testing in Tennessee and South Carolina
- *LRN Results Messenger* 18 labs deployed by May 16
- Planned Implementation in New York State

Current Issues

- Issues with Proxy Servers
- (working on solution, should be forthcoming)
- LDAP Calls blocked at some firewalls
- (work-arounds include locating public key locally) or a web service key retriever)

Where To Get More Information

- ebXML
- www.ebxml.org
- Interoperability
  www.ebusinessready.org
- PHINMS Documentation
  www.cdc.gov/phin
- Request software
- (800) 532-9929 press “2”

Thanks! I'm PHINished!!!